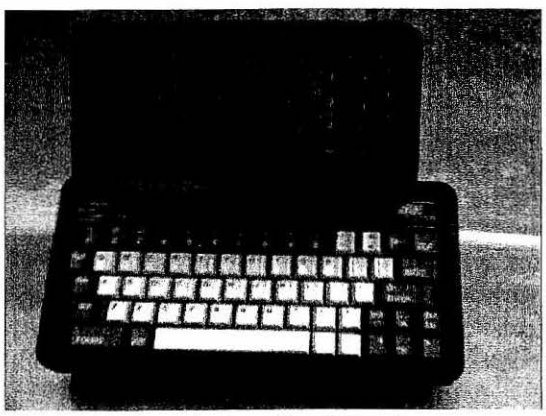
Steve's Scanner Shop

Scanning For MDTs All You Wanted To Know About Them

By Steve Donnell

One of the more obscure and controversial forms of Public Safety(and Business) communications today are found in MDTs(Mobile Data Terminals). Among their many uses, MDTs allow Police to quickly access driver's license records without needing to relay information through a Dispatcher. This provides the Officers in the field fast access to a wide(er) range of information on various criminal suspects, and it helps to leave Dispatchers free for other tasks.

Also, since the information is sent in a digital format, it makes much more efficient use of a radio channel. The radio links used in most early MDT networks were setup on dedicated frequencies licensed to a specific Police Department, or group of departments. In some areas, other departments in a community, such as the fire department were also allowed access to the MDT network.



Top and Center: Older style MDT units

Early MDTs could only permit transmission and reception of text information. This included information about suspected criminals along with requests to respond to different complaints, as is more usually sent by voice from a Dispatcher. Most MDTs also include the ability to send short text messages from an Officer in the field to other mobile units or a Dispatcher.

Newer one with more advanced hardware(terminals) and having more "bandwidth" in the radio links they use can often provide transmission and reception of digital images(photos) or building floor plans and maps. Some MDTs include attachments that can "read" a barcode or magstrip on a Driver's License. I wonder how long it will be before they also include the ability to read the magstrip(or "smart" chip) on a one's credit card, so you can pay for your speeding ticket on the spot. As some can already provide the printed citation given to the violator..

One serious weakness in some early MDT systems was the protocol used in transmission and reception of data contained no "real" encryption protection. Hence it wasn't too long before some enterprising computer programmer was able to figure out how to "decode" the data(text) in MDT signals. This led to the availability of several freeware programs, such as MDT Monitor, showing up that could "read" the message traffic

programs, such as MDT Monitor, showing up that could "read" the message traffic carried on some MDT networks.

In some parts of the world, monitoring of MDT traffic is seen as illegal. Several years ago, an individual was arrested and convicted after he posted transcripts of MDT messages on a Web page. Take this into consideration if you ever even THINK about trying to "read" an MDT signal. As a practical matter, most MDT systems have either upgraded the type of data protocol they use, so that it includes at least some degree of encryption protection, or have moved on to using much more advanced Network that uses a very high level of "embedded" encryption, making any attempt at intercepting this sensitive data a Fool's errand.

Im not a Lawyer, and I don't pretend to be(or play one on TV), but I find it hard to understand how a form of radio transmission that can be displayed using a simple freeware program can be considered by anyone as "private". Even more so if the transmissions take place over as "private"(as opposed to "public" aka Cellular) radio network. In addition, on much lower HF frequencies, there exists a wide range of text format transmissions on both commercial and government channels that can be readily received by shortwave

Hobbyists listening in doesn't seem to raise any eyebrows whatsoever or the fact that "live" scanner (voice)audio can be heard on a number of Web sites without any restrictions. The current legal views on MDT traffic could have implications in the future, as the line between voice and data continues to blur. This is particularly true on some (radio) networks as Motorola Astro, or MaCom's Open Sky, where voice and MDTs use the same channels.

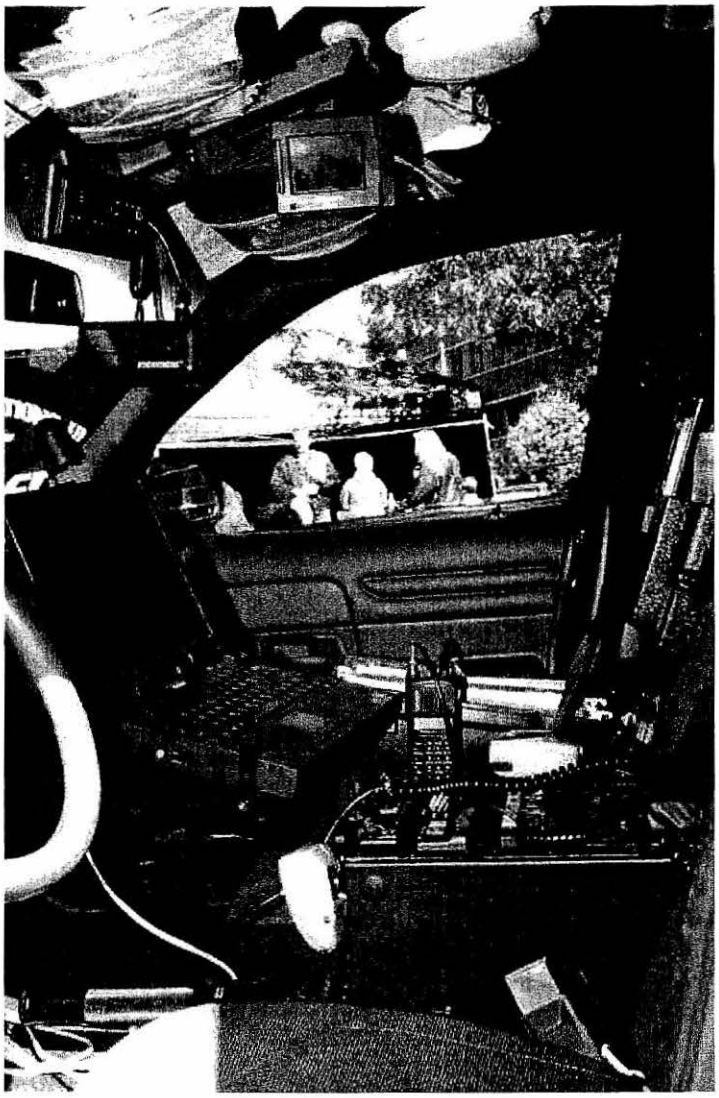
More and more, MDTs are moving to much more advanced "public" networks. Besides as we already mentioned, better security and the ability to send more complex types of data files, using these networks often save money, as a given agency makes use of an existing(rather than building their own) wircless "infrastructure" that carries many types of commercial and individual subscribers.

One very good example of this is that of CDPD(Cellular Digital Packet Data). CDPD has been around for nearly ten years now, although it has taken quite a while for it to fully "mature", as new software applications were developed and enduser hardware has continued to get simpler, smaller, and cheaper. A CDPD typical modem(transceiver) is a small card that can slip into the side of a laptop PC.

We were very fortunate to be a part of the early development and deployment of this service that provides "mobile data" services for a wide range of users and purposes. CDPD makes use of idle frequencies on a given Cellular telephone network. Part of what has helped drive the widespread use of CDPD is that much of the needed infrastructure already exists in the form of towers, building sites and switching network equipment within a given cellular system. Which reduces the total cost of deploying a CDPD network, as opposed to building a wireless data network from scratch.

CDPD is used for much more than just the wireless data link for MDTs. It serves as the wireless "bridge" for anyone needing mobile or portable Internet access. It can be used as the link for nearly any type of remote status and control function. One early application that CDPD was touted for was providing automated refill alerts for vending machines. A project that we were involved with recently, was in using CDPD to serve as the wireless link in remote monitoring of data collected on water levels and flow rates in municipal storm drains.

Although the data sent over a CDPD network incorporates a very high level of encryption against anyone attempting to "eavesdrop". One of things that makes CDPD so flexible is also a vulnerability, in that the end user(PC or other device) is directly connected to the Internet and uses an standard IP address. Though its hard for me to say, this would appear to be a potential problem as to some "hacker" being able to gain access to a device that is remotely controlled or monitored using CDPD, or even a laptop PC in a Police cruiser.



In one recent incident in a large US city, it was found that Police officers were using their wireless laptops to send raciest jokes and pornographic pictures to each other. While I do not know specifically if CDPD was the type of network used in this situation, it would appear that the network was configured in such a way that made internal "oversight" of the messages bing sent somewhat difficult. If the laptops had been setup so as to be ale to only connect into the Police Dept's own network, this would have made it much easier to monitor the types of messages being carried, along with screening of any Internet sites that the laptops had accessed, just as is typically the case within any "wired" business network.

Along with CDPD, there are several other forms of commercial wireless "wide area" networks that can be used for MDT purposes. One of the earliest is the Mobitext network owned by Bell South, which uses dedicated 800 MHZ frequencies. Although much of the usage of this network is for wireless PDAs. Another that has long been a competitor of CDPD is the Ricochet Network developed by a California company called Metricom. Ricochet uses a 900 MHz spread spectrum protocol. It was originally developed to provide a means of remotely reading utility meters.

Although Ricochet can actually provide a somewhat higher speed(data transfer rate) than even CDPD, the future of Ricochet has been in doubt as Metricom has suffered from financial problems. However recently Ricochet appears to have been rescued, in at least some areas of the country. You can be certain that future wireless data networks for both police as well as businesses and individual users will continue evolve into smaller and smaller hardware that provides faster, more reliable connections, and is even easier to use.

NEW @ SCANNINGUSA.COM
We invite our readers to stop at our web site and visit our new Scanning USA forum chat board! Post your scanner related questions, see what is cooking, or post your answer to someone else's question!

Top and Bottom- Most MDTs will look like these